Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2007 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2007

A Theoretical Basis for Defining Internal Control Objectives for Information Systems Security

Sushma Mishra
Virginia Commonwealth University

Gurpreet Dhillon
Virginia Commonwealth University

A Theoretical Basis for Defining Internal Control Objectives for Information Systems Security

Sushma Mishra
Virginia Commonwealth University
mishras@vcu.edu

Gurpreet Dhillon
Virginia Commonwealth University
gdhillon@vcu.edu

Abstract

In the literature it has been argued that individual values play an important role in creation and implementation of internal controls for information systems security. However majority of approaches that help in designing internal control overlook the importance of individual values. In this paper we argue that individual values should form the basis for defining internal control objectives. We propose Value Theory (Catton 1952) as an appropriate basis for conducting the argument. The theory helps in identifying the objectives, which are the guiding principles for design of internal controls. By adopting such a theoretical basis, it will be possible to develop internal controls that are congruent with the organizational objectives.

Keywords: internal controls, information systems security, value theory, value focused thinking, COSO, COBIT

Introduction

Organizational controls are defined as a group of processes that ensure proper sourcing and efficient use of resources to accomplish an organization's objectives (Anthony et al 1989). Controls are fundamental to all organizations (Scott 1995). It is also a central topic of discussion in the management literature (Eisherhardt, 1985). Internal controls are the practices, procedures, policies and responsibility structures in an organization that help in managing risks and protecting information assets (Dhillon, 2001). For a comprehensive security program, controls have to be effective at a formal (e.g. policies & procedures), informal (e.g. norms & behavior), and technical levels (e.g. firewalls & encryption). In the context of information systems security, internal controls are defined as an aggregation of various types of controls deployed effectively at a formal, informal and technical level.

Research in the design of internal control objectives is sparse and not well emphasized. A critical review of the extant literature on controls shows that the research domain is characterized by three problems. First, there is a lack of theoretical basis for creation of internal control objectives. Most of the research in controls is focused on implementation and effectiveness of controls in organizations. Although there is considerable emphasis placed on the nature of controls (Ouchi, 1977; Eisherhardt, 1985), impact of controls on effectiveness of business processes (Kirsch, 1996) and, balance of formal and informal controls (Cardinal et al, 2004), there is little by way of what the control objectives should be and how these can be designed.

Second, there is a lack of guidance on incorporating behavioral and people aspects into the control structures. The importance of informal aspects of controls (such as values, motivations, shared goals of employees) is recognized in the literature but there is a lack of prescribed methods or models in the literature that helps an organization to incorporate these aspects into the control objectives. Third, there is a lack of research in internal controls objectives in the area of information systems security. It is difficult to understand, from the research literature, how organizations arrive at the control objectives for information systems security. Research literature in this area does not provide much insight.

The purpose of this paper is to present a theoretical basis for designing internal control objectives in the context of information systems security. Value theory (Catton, 1952) provides a theoretical basis for understanding individual values about a decision context and value focus thinking (Keeney, 1992) provides a methodology to incorporate such values and create context specific decision objectives. The benefit of using individual values to develop control objectives is twofold: First, there will be a better alignment between individual and organizational goals if the control objectives are created in a "bottom up" approach. Communication in this fashion can reduce the gap between management expectation and employee interpretations about the controls. Second, it will facilitate an environment of shared goals amongst employees, which has long-term implications for an organization's information systems security. In this paper we posit that value theory and value focused approach provide an appropriate theoretical and methodological basis to design internal control objectives for information systems security in organizations. The paper is organized as follows. The next section presents a discussion of various internal control frameworks for design of internal controls. Section three presents a description of theory of value. Understanding a theory from the ontological, epistemological and methodological levels clarifies the conceptual territory. Section four presents an assessment of use of values in research literature. This section is informed by research in management and information systems discipline. Lessons for research in design of internal controls objectives are drawn. Finally conclusions are presented.

Review of current models for internal controls

The various internal control models can broadly be classified into two categories. There are models, which are research based. Such models use a theory to define the requirements. There are also models which are practitioner based. Such models have emerged from best practices of various industries and at times because of mandated regulatory controls.

Research based approaches

Research based models for internal controls have been informed either by the management field or by the information systems discipline. In the management discipline, Ouchi (1977), in his seminal work, argues that controls can be measured along two dimensions: behavior and output of behavior. Several other researchers use the above conceptualization to study controls (Eisenhardt, 1985; Kirsch, 1996, 1997, 2002; Nidumolu and Subramani, 2003). Ouchi (1980) broadly classifies organizational controls into three types: market (information requirement being price), bureaucracy (information requirement being rules) and clan (information requirement being traditions). These modes of controls have been broadly categorized as formal and informal controls. Das and Teng (1998) explore the notion of confidence in strategic alliances and suggest that trust and control are the most important basis for cooperation in alliances.

Research in information systems security identifies internal controls as an integral part of overall information systems security program in an organization (Dhillon 2001). Creation of internal controls and periodic assessment of these controls have been identified as an effective measure for providing adequate security governance (Warkentin and Johnston 2006; Whitman 2003). Management creates internal controls after assessing business risks and prioritizing alternatives to combat such risks (Posthumus and von Solms 2003; Rezmierski et al 2002). Internal controls are established by creating right polices and procedures to meet organizational objectives. Periodic assessment of the effectiveness of internal controls is critical for security governance success (Flowerday and von Solms 2005).

Henson and Lee (1992) study the control relationship between project managers and team members for a design team for software development. The findings suggest that high performing teams show high process control by the project leaders and high outcome control by the team members. They also suggest a positive

correlation between high control over the team and performance for the team in the context of project development. Orlikowski (1991) investigates the changes in forms of control and types of organizing due to information technology use in business processes. The results indicated that use of information technology reestablished the prevalent form of organizing and enhanced the current control structures. Use of information technology creates a facilitative environment and enhances flow of knowledge in the organization. Hensen and Hill (1989) study the control architectures and concerns associated with EDI. Audit considerations in the EDI environment and related audit tools, are also outlined in this research.

Clearly research in the area of organizational controls for information systems and security is limited. While some researchers have highlighted the importance of coordination among team members, others have focused on trust. Apparently there is limited focus on how the right kind of controls has been configured such that they are in sink with the organizational objectives.

Practitioner based approaches

Information Systems Audit and Control Association (ISACA) define internal controls as "Policies, procedures, practices and organizational structures put in place to reduce risks (pp. 51)". Based on information systems security perspective, controls can be classified as three types (ISACA, 2004):

- Preventive controls: attempts to prevent potential problems through various preventive measures such as segregation of duties, use of well designed documents and use of access controls.
- Detective controls: attempts to find errors and anomalies in routine business processes such that breaches are detected. Examples include checkpoints in production job, duplicate checking of calculations, audit trails.
- Corrective controls: attempts to minimize the impact of occurred exposures and identify the cause of problems such that future occurrences can be minimized. Examples include contingency planning, backup procedures.

There are the three most widely used frameworks for internal controls assessment in organization. Each on them is briefly discussed below:

Control objectives for Information and related technology (COBIT) is industry's leading framework for information systems control objectives and related good practices (ISACA, 2004). COBIT primarily guides organizations for better information technology governance, control structures and means of providing assurance. It divides IT processes into four domains and 34 broad control objectives through the entire business process cycle.

COSO stands for the "Committee of Sponsoring Organizations of the Treadway Commission," a nonprofit commission that in 1992 established a common definition of internal controls. The COSO framework views internal controls as consisting of the following five interrelated components: *control environment* (**"**setting the tone" of the organization or the broad ethical values of the management), *risk assessment* (process of identifying and mitigating risk activities in the organization), *control activities* (identifies internal control activities to mitigate risks defined in prior domain i.e. risk assessment), *information and communication* (create reporting processes that help in assessment of the technology environment), *monitoring* (assessment of the quality of a company's internal control over time). COSO and COBIT frameworks are widely used as guidelines for Sarbanes-Oxley compliance, systems audit in organizations and also for information technology governance purposes.

ISO 17799 provides high-level principles for comprehensive information system security that relies on either legal requirements or generally accepted best practices. Measures based on legal requirements include: protection and nondisclosure of personal data, protection of internal information and protection of intellectual property rights. It provides guidance to information security professionals for implementing information security programs. It is widely used as a basis for developing security standards and management practices within an organization and helps in improving reliability of information security in inter-organizational relationships. The best

practices endorsed by the above framework need critical thinking before implementation on the part of the management.

Emergent issues: Establishing a need for the theory

An assessment of the contemporary frameworks for internal controls suggests two problems with the use of these models. First, all the existing frameworks reviewed are atheoretical based on experiences of the originators of the models and derived from best practices in the industry. The guidelines are mechanistic with "one size fits all" approach. Use of the principles suggested in these frameworks need to be tailored and prioritization. Second, none of the above frameworks provide guidelines specific to creation of objectives of internal controls for information systems security. Either the focus is too broad covering much more than security or the guidance is about using specific controls. Review of the research literature in internal controls for organizations does not shed much light on the process of creation of internal control objectives for information systems security. Internal controls for information systems security literature lack the rigor of a theory to guide research in this area. Research in information systems security area does not provide an appropriate theoretical basis to design internal controls for security. The analysis of internal control design, both in research and practioner worlds, shows a need for a theoretical basis for internal controls.

Value theory: philosophical underpinnings

A theoretical platform has an implicit ontological and epistemological position. Methodology and method, used with a particular theory for research, should be consistent with the philosophical assumptions of the theory. This section presents the ontological and epistemological position of the value theory and discusses an appropriate methodology and method to study values.

Ontological and Epistemological position

Catton (1952) proposes "value theory" as a theory of valuing behaviors. Value theory states that an individual's preferential behavior shows certain regularities and this pattern can be attributed to some standard or code, which persists through time. Values provide a basis by which people can order their intensities of desiring various desiderata (something desirable). Given the available choices, people make preferences based in their values. In an organizational context, knowledge of such preferences of individuals provides a context for managerial decision-making.

According to Burrell and Morgan (1979), "all theories of organization are based on a philosophy of science and a theory of society (p. 1)". Ontological position of value theory is similar to the ontology of research belonging to interpretive paradigm (Burrell and Morgan, 1979) in research. Ontology is the position or the stance that a researcher takes on objects in the world. Ontology is used commonly to refer to study of being. Interpretive research considers our knowledge about the world as a "social construction of reality". As Berger and Luckmann (1973) observe "Society exists as both objective and subjective reality, any adequate theoretical understanding of it must comprehend both these aspects (pp. 129)." The above conception is similar to the conception of Habermas, who claims that there are three different types of world: first is objective, second is subjective and the third world is the social world that has objective, legitimate and socially accepted norms and structures (Habermas, 1984). Value theory perceives values as object of the socially constructed world. Values, according to "social construction" perspective, have an objective presence outside the minds of the people, and shape their lives and actions. According to Gregor (2006), theory can have an existence separate from the subjective understanding of individual researchers. Adler (1956) claims that values are internal to humans and cannot be directly observed or measured.

Lee (2004) calls epistemology as a broad and high-level outline of the reasoning process by which a school of thought performs its empirical inquiry. The term epistemology is derived from the Greek episteme ("knowledge") and logos ("reason"), and accordingly the field is sometimes referred to as the theory of knowledge. The epistemology of value theory suggests that individuals develop a pattern of relationships, which serves as symbolic forms representing the structuring process of preferences amongst people. Epistemologically, value theory facilitates in gaining a deeper understanding of conformity issues in organizations and provides insight into individual's objectives and goals. In the interpretive paradigm, "the

goal of theory building is to generate discussions, insights and explanations of events so that the system of interpretations and meaning, and the structuring and organizing processes, are revealed (Gioia and Pitre, 1990)". Research in information systems discipline entails knowledge of properties of physical objects (such as machines) and knowledge of human behavior (Gregor, 2006). Value theory emphasizes on eliciting and identifying the underlying values of the people, an inherent part of information systems.

Keeney (1992) argues that values are guiding principles to evaluate the desirability of a particular consequence. Value focused thinking provides a way of generating innovative solutions. The decision maker is not constrained by "what can be done" or "what is usually done" under similar conditions. The thought process revolves around "what is important" and "how can it be done". Considering the values of decision makers in a context of a problem provide solutions, which have higher probability of being successful.

Methodological Position

Methodology provides specific guidelines to perform empirical investigation for a research problem. For a particular ontological and epistemological position, there could be various methodologies to conduct a research. Depending on the choice of methodology, there could be many ways in which a theory can be empirically tested i.e. an epistemology can have many methodologies for validation proposes. Values as a construct can be empirically studied (Catton, 1954). Measurability of any class of values is possible and depends on researcher's ingenuity in creating techniques or ways for obtaining discriminal responses to items capturing the value construct. Catton (1956) empirically validated his argument that individual values are suitable for empirical research. Keeney (1992) provides a methodology known as value focused approach that lends itself for suitable assessment of values.

Value focused approach is provides a way to elicit the individual values in creating a common denominator for a multi criteria decision-making context. Method is the instrument through which actual data is collect in a study. A particular methodology of conducting the research, there could be multiple ways of collecting actual data i.e. there could be many methods employed to obtain data. Keeney (1992) proposes semi-structured interviews as one of appropriate method of collecting data in this methodology. According to value focused approach, the best way to understand underlying values about any issue is to ask people what is important to them in the particular context and why is it important (Keeney, 1999). For a particular research problem, personal values of people regarding the research question are elicited. Keeney suggests a three step process for using value focused approach in an inquiry. These steps are:

Elicit and create a comprehensive list of personal values underlying the problem: the aim of the researcher at this stage is to elicit the underlying values of respondents through probing. The process of identifying the values begins with interviewing people. A guiding definition is provided about the research context, scenarios are projected and interviewees are asked to provide examples to demonstrate their choices. Direct questions about values might not be useful as values are difficult to surface and more difficult to express explicitly. The personal values surfaced through the interview session are listed.

Obtain a common denominator or common objectives: a list of objectives corresponding to the values of respondents is generated at this stage. The data collected (transcripts of the interviews) are converted into a common form at this stage. These common denominators give rise to values. These values provide the objectives, when a verb is added to them. The values that are listed are objects and ways to achieve this object becomes the objective. The verb form of the values thus created could be termed as the objective of that object. An objective has three features: a decision context, an object and a direction of preference (Keeney, 1992).

Classify the objectives as fundamental for decision context or as means objectives: this is the final step in value-focused approach and the end result is a network of means and fundamental objectives. Classification of all the objectives formed is done and all the objectives clusters are divided two categories, "means" or "fundamental". Depending on the role of a category in a decision context, a category can be "means" to the decision or an "end" to the decision objective for the problem context. An objective that leads to another objective for being considered in decision-making is a *means* objective whereas an

objective which is fundamental and important in its own right, in a decision making process is called fundamental objective. This is primarily done through performing a *why is this important* (WITI) test for each of the objective (Keeney, 1992).

Value theory: A basis for studying internal controls

This section presents a discussion on the use of "values" in information systems research. The discussion is presented in three parts. First part presents a discussion on how values have been studied in information systems security research. Second part presents a discussion on how values have been used in management discipline. Third part presents the lessons derived from such usage for internal control research.

Concept of values in IS Security Research

Research in information systems security recognizes the importance of individual values in successful security programs. Von Solms (2001) recognizes that information systems security policies and controls do not have human considerations. Successful implementation of the controls and polices is facilitated when individuals are able to align their value system with that of the management. Researchers argue that if there is a misalignment between individual and organizational goals, there are greater security threats to information systems from the insiders in the organization (Loch and Conger, 1996; Magklaras and Furnell, 2005; von Solms, 2001; Stanton, 2005). Dhillon and Torkzadeh (2006) study the values of employees for information systems security in organizations. The employees should be treated as owners of information assets (Adams and Sasse, 1999) such that responsibility and accountability, on the employee's part is enhanced.

Concept of values in organizational research

Organizational research has long emphasized the importance of studying personal and group values in organizational settings. Davis (1958) calls management philosophy as the philosophy of individualism and claims, "management philosophy emphasizes the concepts of delegation, decentralization, individual initiative and individual accountability (p. 39)." In a study to understand the impact of personal values on organizational decisions, Senger (1971) measured personal value orientations by using a value scale. The values provided the structure for the scale and a semantic differential technique was used as a scaling device. Senger's study suggests that "personal value structures and systems of preference ordering used by decision-makers could lead to more useful decision models better able to predict choice behavior (p. 422)." Research in authority of management in organizations studies value systems of individuals. Authority depends on its acceptance by those it intends to direct. Hence any emerging pattern of authority must be consistent with the values of individuals it is directed to and embody the emerging ideals, purposes and values of individuals (Albanese, 1973). A manger's effectiveness is determined by the values of his associates and the pattern of authority they attempt to implement (Albanese, 1973).

Lessons for studying internal controls

Controls are the set of mechanisms designed in order to motivate individuals to attain desired objectives (Kirsch, 2002). Management conveys its philosophy and goals through the control objectives to the employees. Creation of internal control objectives for information systems security through individual values of the employees facilitates the understanding of such objectives for better security results. Individual beliefs of employees shape the interpretation and hence the success of all security measures in an organization (Magklaras and Furnell, 2005; McHugh and Deek, 2005). The informal controls help in effectively reaching out to people and conveying management's ideas (Adams and Sasse, 1999; Schultz, 2002). Employee's behavior, especially for security issues, is critical for an organization. User sophistication, social engineering and end user behavior are well-researched constructs in security literature (Loch and Conger, 1996) and the findings emphasize the importance of individual belief system in security management.

Research in designing internal controls for information systems security could use value theory as a theoretical basis for studying issues in this domain. Values provide decision objectives around which internal controls can be designed in a proactive fashion. Existent models for internal controls show reactive ways of dealing with internal control threats. Value theory provides a means to incorporate such values in

the design process. The process of creating control objectives from value theory is demonstrated in the figure 1 below.

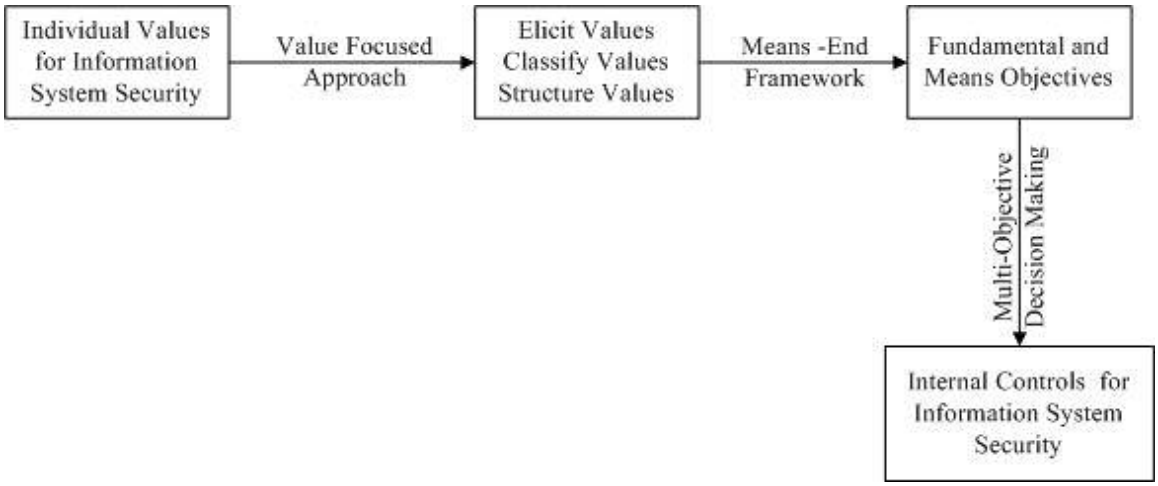

Figure 1. Designing internal control objectives from individual values for information systems security

The domain of designing internal control objectives for information systems security is plagued with two problems. Firstly, research in this area (management, information systems and information systems security) does not provide a theoretical basis to design internal control objectives. There is a lack of guidance, on how to actually design internal control objectives. Secondly, practitioner based models provide generic control objectives and controls based on experience but do not suggest ways of actually creating these objectives. These models are atheoretical, broad in scope and have a "one size fits all" approach.

This paper proposes using value theory and value focused approach to create internal control objectives for information systems security. There are three benefits of using this approach for internal controls design. First, this approach incorporates the fundamental values of people about internal controls and the objectives thus created are grounded in people's values and beliefs. Values are more fundamental to decision context than alternatives available (Keeney, 1992). Since employees' security behavior depends of the personal values and standards of conduct (Leach 2003), the employees can relate better to the controls (being a reflection of their core values) and information systems security program can be better governed. Second, the proposed approach provides a theoretical basis for designing internal control objectives and thus makes a theoretical contribution to the discipline on information systems security and management. There is a limited research in the area of design of internal control objectives and using value theory and value focused thinking to create control objectives fills this gap. This theoretical basis could direct research efforts in this relatively unexplored area and benefit the body of knowledge in related disciplines. Third, the practitioner community could benefit from the proposed approach that leads to a means-end framework of internal control objectives. Internal control objectives, rooted in personal values of employees, would lead to more robust and proactive design of internal controls. Security behavior of the employees would be in accordance with management's expectation which is conveyed through internal controls objectives.

Conclusion

Design of internal control objectives can be studied from value theory perspective. Using value-focused approach provides a methodology to illicit, interpret and utilize individual values for better design of internal controls for security purposes. A theoretical lens, such as value theory, is required for rigorous investigation of issues in designing internal controls objectives. Use of value theory to understand the

design aspects of internal controls for information systems security can be attributed as a theory building exercise. Creation of a means-end framework for internal controls in information systems security context helps in identifying the objectives for decision making. The empirically validated means-end framework would ground the objectives in organizational context and facilitate adoption of such control objectives.

Internal control objectives, created from the values of individuals, provide a bridge between management's vision of organizational security and employee's perception of adequate means of achieving the desired security state. Analyzing the extant literature about internal controls and the widely used internal controls models in research and practioner world, a case for using value theory in design of internal controls is made. The process of creating controls from individual values is explained in figure 1. Contributions from this research are discussed.

References:

Adams, A. and Sasse, M.A. "Users are not the enemy, Association for Computing Machinery," *Communications of the ACM* (42:12) 1999, pp 40-46.

Adler, F. "The Value Concept in Sociology", *The American Journal of Sociology*, 1956, 62(3), pp. 272-279

Albanese, R. "Criteria for Evaluating Authority Patterns," *Academy of Management Journal*, 16 (1), Mar 1973, pp. 102-111

Anthony, R., Dearden, J. and Bedford, N. M. *Management Control Systems*, 6th edn Homewood, III: Irwin, 1989.

Berger, P.L. and Luckmann, T. The Social Construction of Reality: A Treatise in the Sociology of Knowledge, Garden City, NY: Anchor Books.

Brown, W. and Nasuti, F. "Sarbanes-Oxley and Enterprise Security: IT Governance - What It Takes to Get", *Information Systems Security,* 14(5), Nov/Dec 2005, pg. 15-28

Burrell, G. and Morgan, G. *Sociological paradigms and organizational analysis* Brookfield, VT: Ashgate Publishing, 1979

Cardinal, L.B., Sitkin, S.B. and Long, C.P. "Balancing and Rebalancing in the Creation and Evolution of Organizational Control," *Organization Science* (15:4) 2004, pp 411-431

Catton, W. "Exploring Techniques for Measuring Human Values", *American Sociological Review*, 1954, 19 (1), pp. 49-55

Catton, W. "A Retest of the Measurability of Certain Human Values", *American Sociological Review*, 1956, 21(3), pp. 357-359

Catton, W. "A Theory of Value", *American Sociological Review*, 1959, 24(3), pp. 310-317

Das, T.K and Teng, B.S. "Between Trust and Control: Developing Confidence in Partner Cooperation in Alliances,", Academy of Management Review (23:3) 1998, pp 491-512

Davis. R. "The Philosophy of Management", *Academy of Management Journal*, Dec 1958, pp. 37-40

Dhillon, G. "Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns." Computers & Security 20(2): 165-172.," *Computers & Security* (20:2) 2001, pp 165 - 172

Dhillon, G. and Torkzadeh, R. “Value-focused Assessment of Information Systems Security in Organizations”, *Information Systems Journal*, Vol. 16 (3), 293-314

Eisenhardt, K. “Control: Organizational and Economic Approaches,” *Management Science,* (31:2), 1985, pp 134-149

Flowerday, S. and von Solms., R. "Real-time information integrity = system integrity+ data integrity +continuous assurances," *Computers & Security* (24) 2005, pp 604 – 613

Gioia, D. and Pitre, E. “Multiparadigm Perspectives on theory Building”, Academy of Management. The Academy of Management Review, 15(4), Oct 1990, pp. 584-602

Gregor, S. “The nature of theory in information systems”, *MIS Quarterly,* (30:3), 2006, pp. 611-642

Hansen, J. and Hill, N. “Control and Audit of Electronic Data Interchange”, MIS Quarterly (13:4) 1999, pp. 403-413

Information Systems Audit and Control Association (ISACA)(2004). *CISA Review Manual, 2004 Edition*. Rolling Meadows, IL: ISACA.

Keeney, R. *Value-focused thinking: a path to creative decisonmaking*. Harvard University Press. Cambridge, Massachusetts, 1992.

Keeney, R. “The Value of Internet Commerce to the Customer”, *Management Science.* Vol. 45, No. 4, 1999, pp. 533-542

Kirsch, L.J. “Deploying Common Systems Globally: The Dynamics of Control,” Information Systems Research (15:4) 2004,

Leach, J. “Improving user security behaviour”, Computers& Security, (22:8), 2003, pp.685-692

Lee, A. “Thinking about Social theory and Philosophy for Information Systems”. In *Social Theory and Philosophy for Information Systems,* J. Mingers and L. Willcocks (eds.), John Wiley & Sons, Ltd, Chichester, England, 2004, pp. 1-26.

Loch, K. and Conger, S. "Evaluating Ethical Decision Making and Computer Use," *Communications of the ACM* (39:7), July 1996, pp 74-83.

Magklaras, G. and Furnell, S. "A preliminary model of end user sophistication for insider threat prediction in IT systems," *Computers & Security* (24) 2005, pp 371-380.

McHugh, J and Deek, F. D. "An Incentive System for reducing Malware Attacks," *Communications of the ACM* (48:6), June 2005, pp 94-99

Orlikowski, W. “Integrated information environment or matrix of control? The contradictory implications of information technology”, *Accounting, Management and Information Technologies,* (1:1), 1991, pp. 9 42

Ouchi, W.G. “The Relationship between Organizational Structure and Organizational Control,” *Administrative Science Quarterly* (22:1) 1977, pp 95-113

Ouchi, W.G. “Market, Bureaucracies and Clan,” *Administrative Science Quarterly* (25:1) 1980, pp 129-141

Posthumus, A. and von Solms, R.V. "A framework for the governance of information security," *Computers & Security* (23) 2004, pp 638-646.

Rezmierski, V.E., Seese, M.R and St. Clair II, N. "University systems security logging: who is doing it and how far can they go?" *Computers & Security*, 21(6), pp 557-564, 2002

Schultz, E. "A framework for understanding and predicting insider attacks," in: *Compsec* London, 2002.

Scott, W.R. (2005). *Organizations: Rational, Natural and Open Systems* (5th Edition). Englewood Cliffs, N.J.: Prentice-Hall.

Senger, J. "Managers' Perception of Subordinates' Competence as a Function of Personal Value Orientation", *Academy of Management Journal*, Dec 1971, pp. 415-423

Stanton, J. and Stam, K. "Analysis of end user security behaviors," *Computers & Security* (24) 2005, pp 124-133.

Von Solms, B. "Corporate Governance and Information Security," *Computers & Security* (20:3) 2001, pp 215-218.

Warkentin, M. and Johnston, A. (ed.) *IT Security Governance and Centralized Security Controls* Idea Group Publishing, Hershey, P.A., 2006

Whitman, M. "Enemy at the Gate: Threats to Information Security," *Communications of the ACM* (46:8) 2003, pp 91-95.